RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: CIT-M05

# Navigating Systemic Cyber Risk: Identifying Blind Spots in Supply Chains

Dr. John D. Johnson
President & Founder
Docent Institute

Colonel JC Vega, USA (Ret)
Advisory & Founder
Executive Security Advisors

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

# We Live in an Uncertain World

"There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know."

Donald Rumsfeld, U.S. Secretary of Defense, February 12, 2002

# We Live in a World With Increasing Risk

## Increasingly:

- Interconnected
- Complex
- Global
- Relying on advanced technology
- Creating more data
- Tightly coupled interactions
  - In search for efficiency, systems may become less resilient to failure

## Increasing Risk:

- More adversaries have access to sophisticated attack tools
- Increasing system dependencies, often undocumented
- Mix of OT and IT environments
- Lack of redundancies & segmentation
- Legal, Economic, Geopolitical
- Different cultures, different ethics

# Systems of Systems (SoS)

## Networks of interconnected systems

A collection of independent & operational systems that:

- Function collaboratively
- Retain individual autonomy
- Interact dynamically
- Exhibit emergent behavior
- Are distributed
- Evolve over time

SoS Archetypes and Risk

- SoS
  - Complex Systems of Systems (CSS)
  - Complex Adaptive Systems (CAS)
- Risk
  - Global Systemic Risk
  - Systemic Cyber Risk

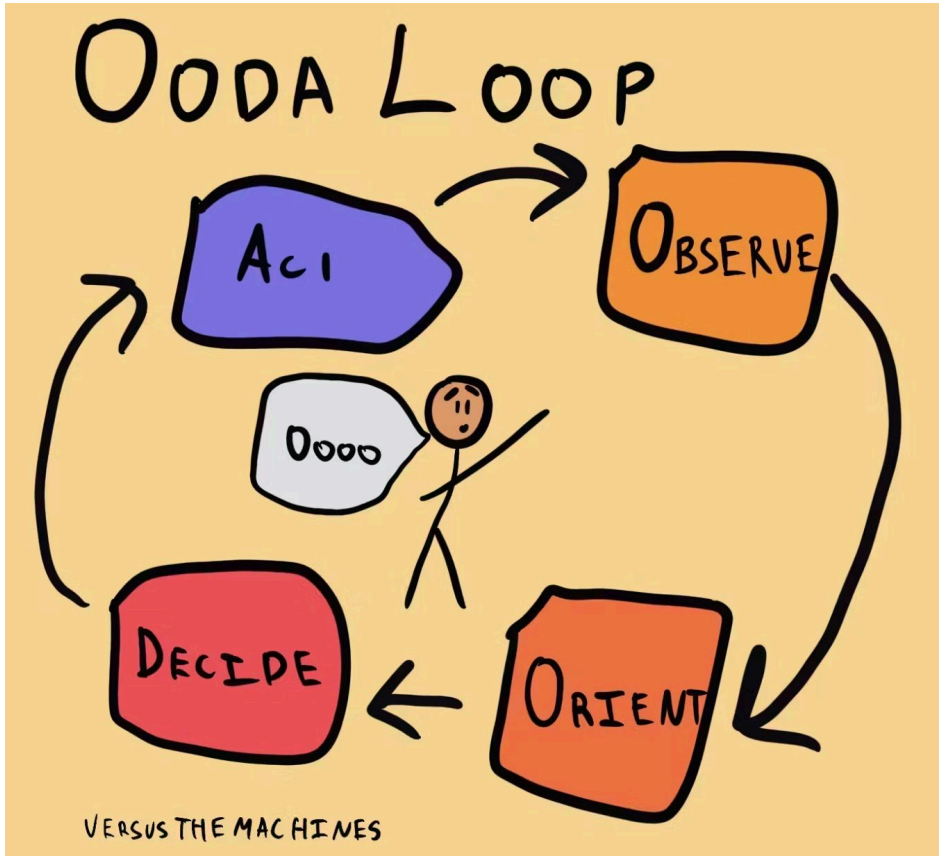
# Complex Systems

## Attributes

- Inputs
- Outputs
- Feedback
- Interconnected & Interdependent

> Complex systems are prone to "normal accidents" due to unexpected interactions.
> – Charles Perrow

Simple:

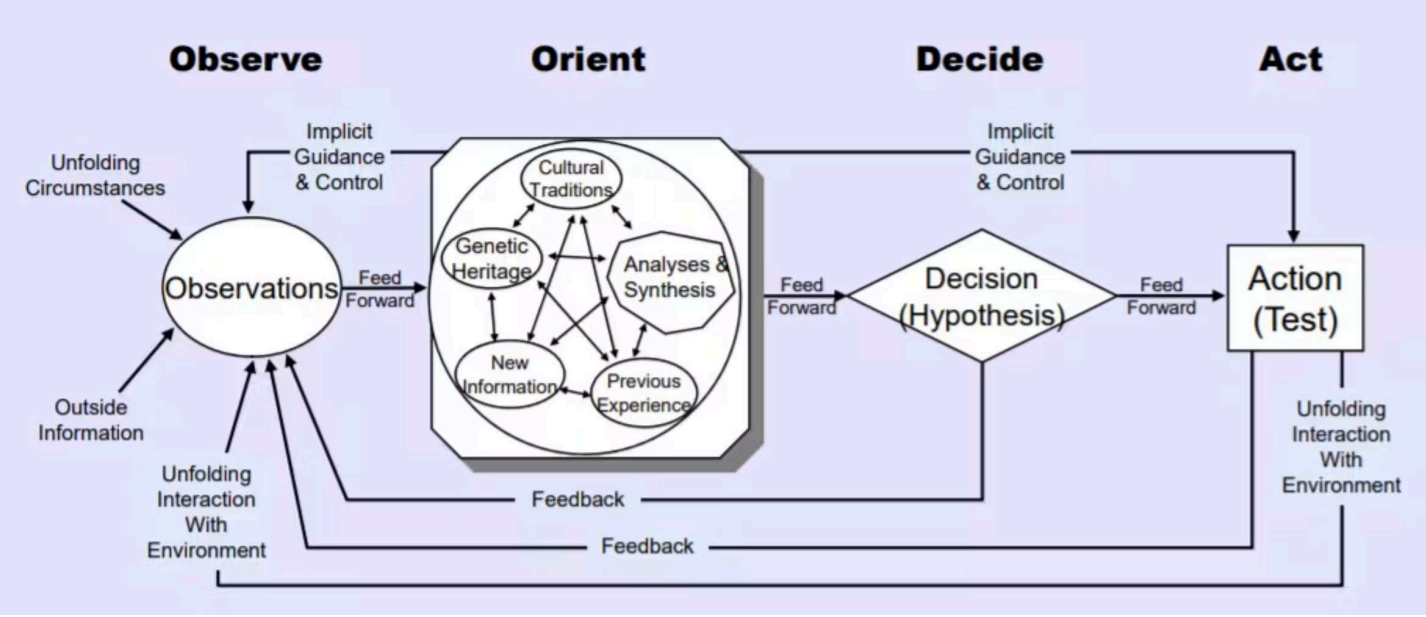


# Complex Systems of Systems

## Attributes

- Multiple Independent Systems
- Distributed Control
- Emergent Behavior
- Interconnected & Interdependent
- Complex Interactions
- Difficult to Predict

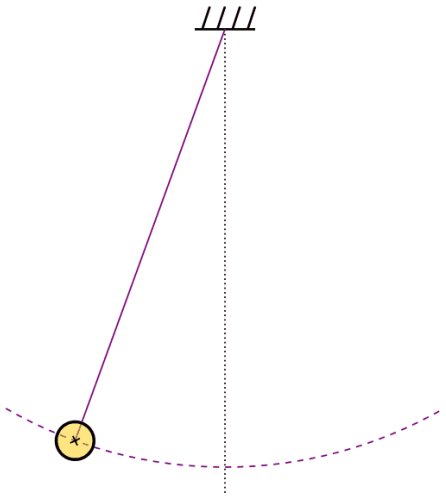
Not So Simple:



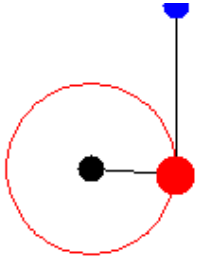
# Complex, not just complicated

Complex interactions create new dynamics that cannot be explained solely by the behavior of its constituents

Simple System: Predictable



Complex System: Unpredictable



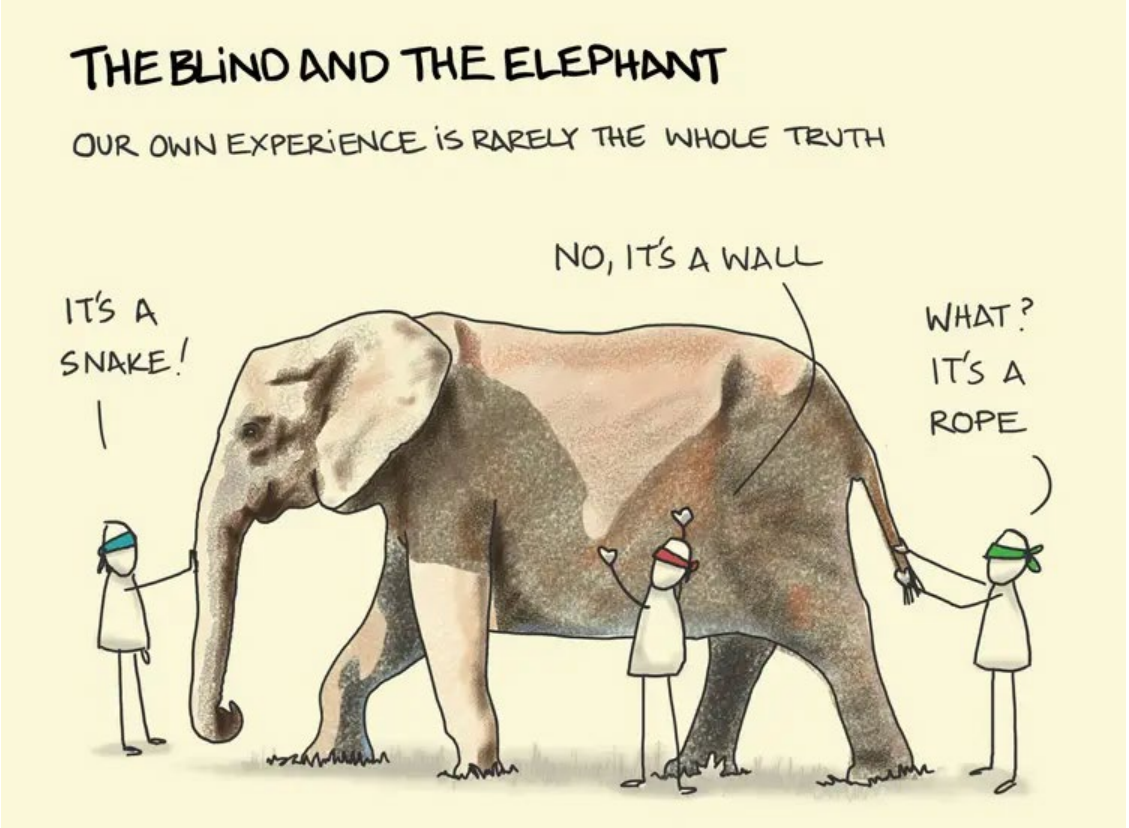
# Complex Adaptive Systems (CAS)

Connected networks of interconnected agents, each with their own unique characteristics & capabilities

CAS are characterized by:

- Ability to self-organize, adapt & evolve
- Order is emergent vs predetermined
- The system's history is irreversible
- Outcomes are often unpredictable

"No One Sees the Whole Elephant"

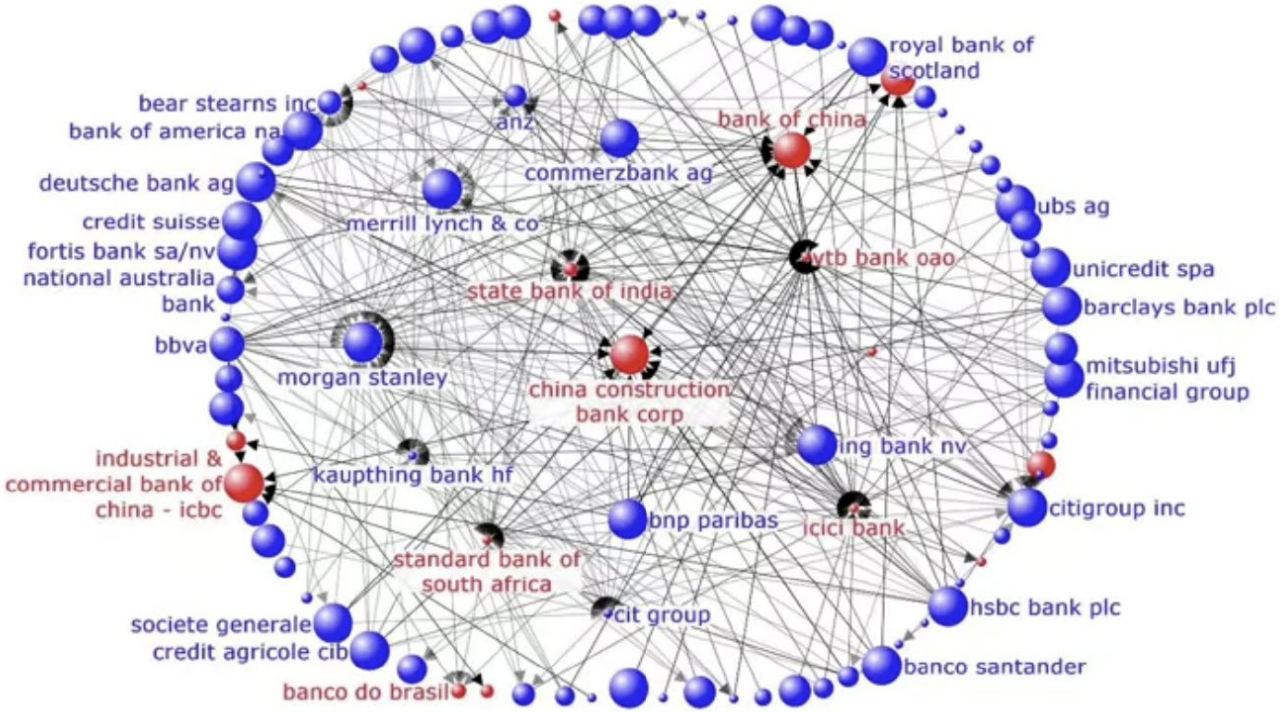


# No Single Mind Holds the Map

Complex networks made of many nodes, with many connections & interactions

**In Nature:** The large-scale structure of the flock is an example of an emergent property.

**Global Banking Network:** No individual has complete knowledge of the state of the network at any time.




DOCENT INSTITUTE

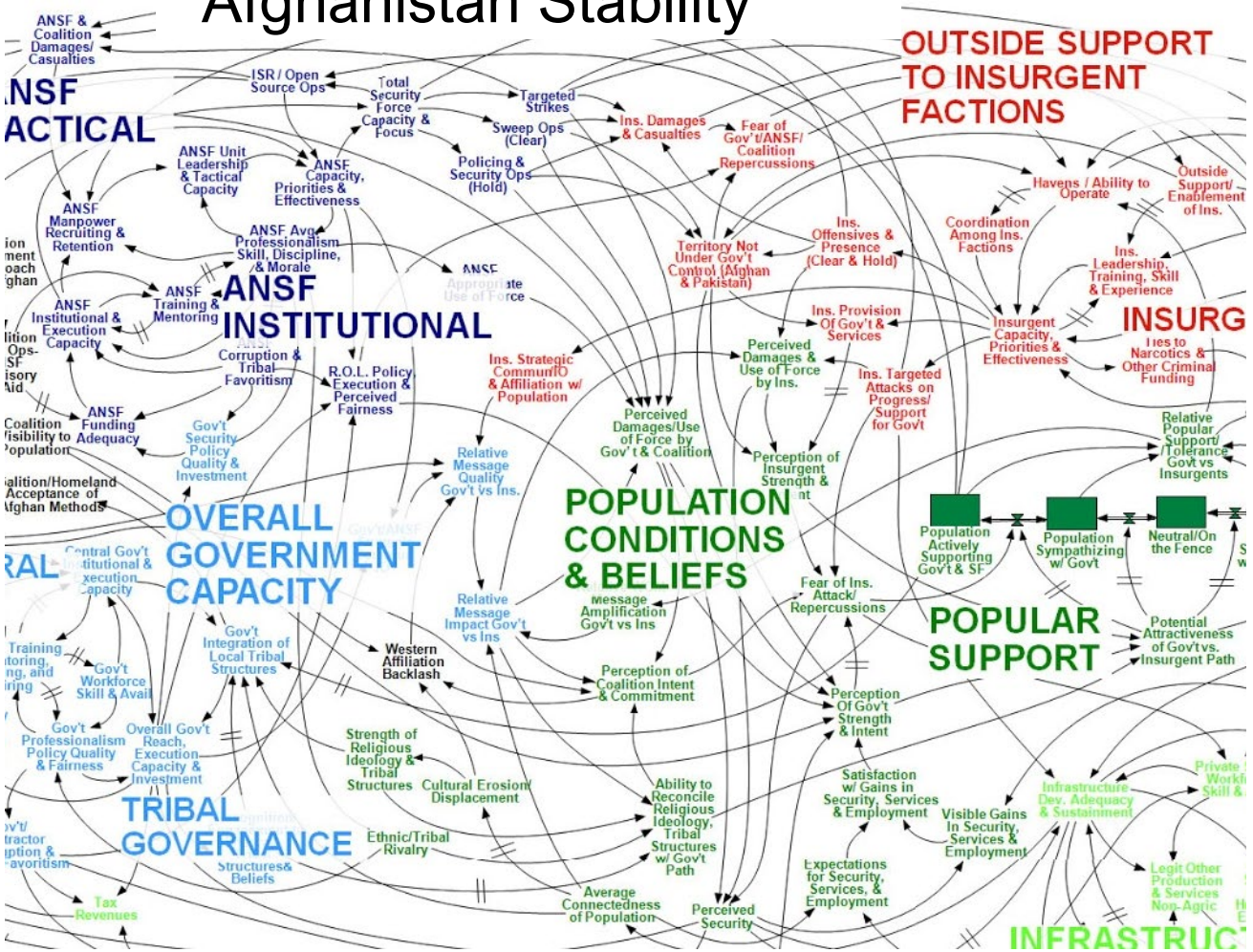
EXECUTIVE SECURITY ADVISORS

# CAS and Supply Chains

## Observations
(General Stanley McChrystal)

- Lack of Determinism
- Complex Activity
- No Center of Gravity or Key Nodes
- Unpredictable
- Challenging to Define the Problem “Unknown Unknowns”

## Afghanistan Stability

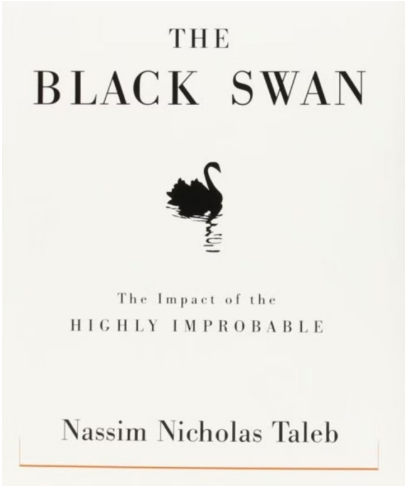

OUTSIDE SUPPORT TO INSURGENT FACTIONS
ANSF TACTICAL
ANSF INSTITUTIONAL
OVERALL GOVERNMENT CAPACITY
POPULATION CONDITIONS & BELIEFS
POPULAR SUPPORT
TRIBAL GOVERNANCE
INSURG
INFRASTRUC
ANSF & Coalition Damages/ Casualties
ISR / Open Source Ops
Total Security Force Capacity & Focus
Targeted Strikes
Sweep Ops (Clear)
Policing & Security Ops (Hold)
Ins. Damages & Casualties
Fear of Gov't/ANSF/ Coalition Repercussions
ANSF Unit Leadership & Tactical Capacity
ANSF Capacity, Priorities & Effectiveness
ANSF Manpower Recruiting & Retention
ANSF Avg Professionalism Skill, Discipline, & Morale
ANSF Training & Mentoring
ANSF Institutional & Execution Capacity
Territory Not Under Gov't Control (Afghan & Pakistan)
Ins. Offensives & Presence (Clear & Hold)
Havens / Ability to Operate
Outside Support/ Enablement of Ins.
Coordination Among Ins. Factions
Ins. Leadership, Training, Skill & Experience
Insurgent Capacity, Priorities & Effectiveness
Ties to Narcotics & Other Criminal Funding
Ins. Provision Of Gov't & Services
Perceived Damages & Use of Force by Ins.
Ins. Targeted Attacks on Progress/ Support for Gov't
Corruption & Tribal Favoritism
R.O.L. Policy Execution & Perceived Fairness
Ins. Strategic Comm/IO & Affiliation w/ Population
ANSF Funding Adequacy
Gov't Security Policy Quality & Investment
Relative Message Quality Gov't vs Ins.
Perceived Damages/Use of Force by Gov't & Coalition
Perception of Insurgent Strength &
Relative Popular Support/ Tolerance Govt vs Insurgents
Population Actively Supporting Gov't & SF
Population Sympathizing w/ Govt
Neutral/On the Fence
Fear of Ins. Attack/ Repercussions
Message Amplification Gov't vs Ins
Relative Message Impact Gov't vs Ins
Central Gov't Institutional & Execution Capacity
Gov't Integration of Local Tribal Structures
Western Affiliation Backlash
Perception of Coalition Intent & Commitment
Perception Of Gov't Strength & Intent
Potential Attractiveness of Gov't vs. Insurgent Path
Training
Gov't Workforce Skill & Avail
Gov't Professionalism Policy Quality & Fairness
Overall Gov't Reach, Execution Capacity & Investment
Strength of Religious Ideology & Tribal Structures
Cultural Erosion/ Displacement
Ethnic/Tribal Rivalry
Ability to Reconcile Religious Ideology, Tribal Structures w/ Gov't Path
Satisfaction w/ Gains in Security, Services & Employment
Visible Gains In Security, Services & Employment
Infrastructure Dev. Adequacy & Sustainment
Expectations for Security, Services, & Employment
Legit Other Production & Services Non-Agric
Tax Revenues
Structures& Beliefs
Average Connectedness of Population
Perceived Security

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

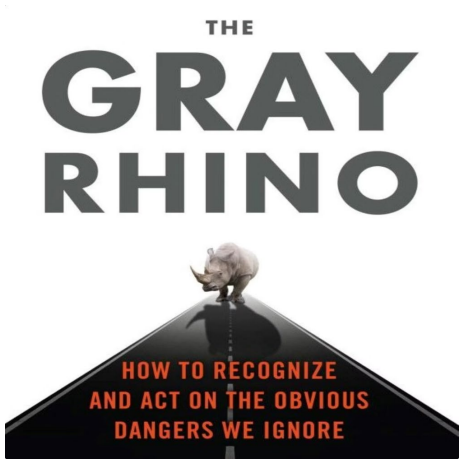
# Failures in Complex Adaptive Systems Can Lead to Significant & Widespread Impacts

## Black Swans




- Unpredictable & Rare
- Significant & Widespread Impact
- Requires
  - Thinking beyond conventional data and models
  - Scenario Planning
  - Stress Testing

## Gray Rhinos




- Predictable
- Preventable
- Manageable
  - Proactive Risk Assessments & Threat Modeling
  - Mitigation Strategies
  - Address early and often
  - Often dismissed due to confirmation bias

DOCENT INSTITUTE

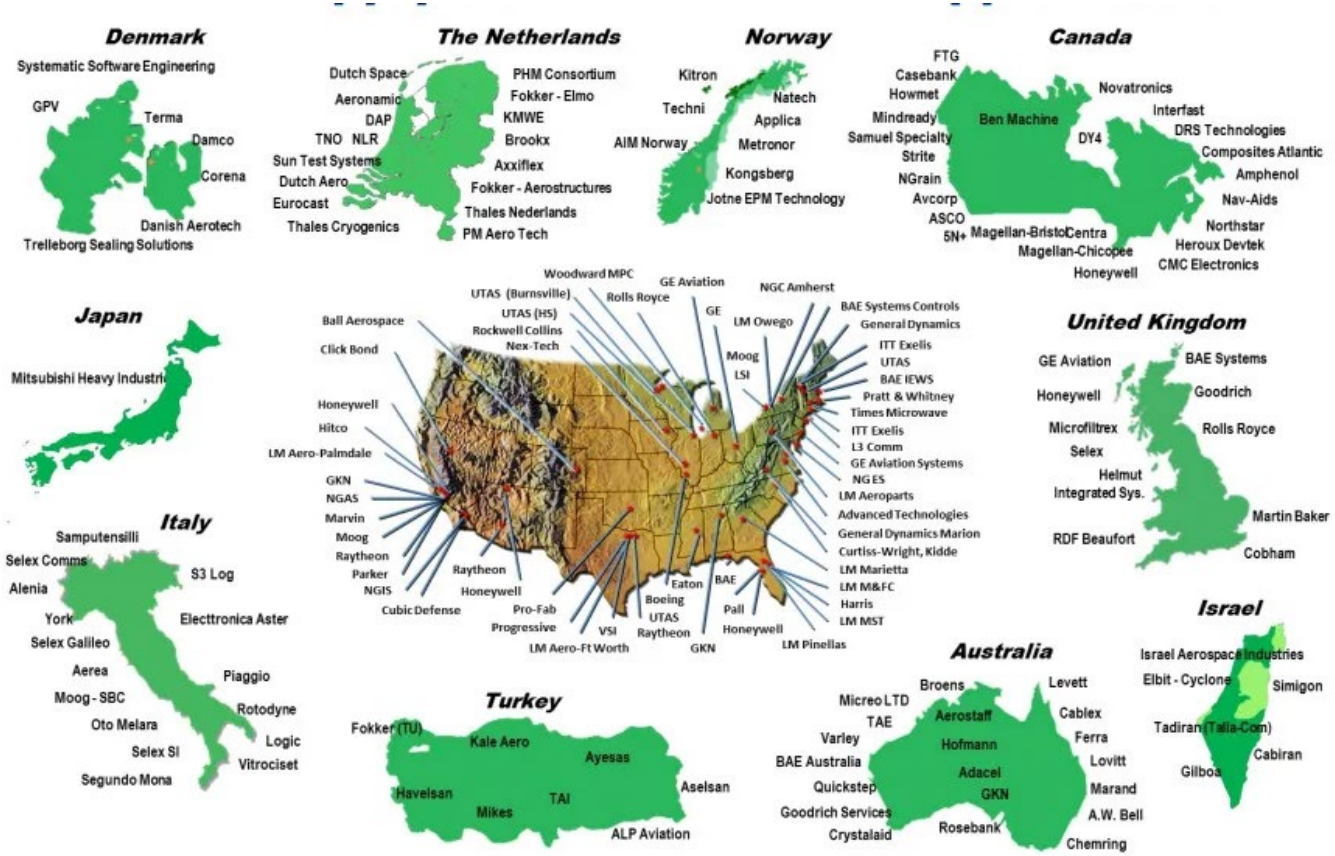
EXECUTIVE SECURITY ADVISORS

# Global Systemic Risk

## Attributes

- Tightly Coupled Interactions
  - Increased risk of catastrophic failures
- Continuous Flow of Data, Information, Artifacts, Services, People
- Efficiency (E) vs Resiliency (R)
  - Integration vs Dependency
  - Redundancy vs Survivability
  - Stability vs Fragility vs Speed

## F-35 Global Supply System

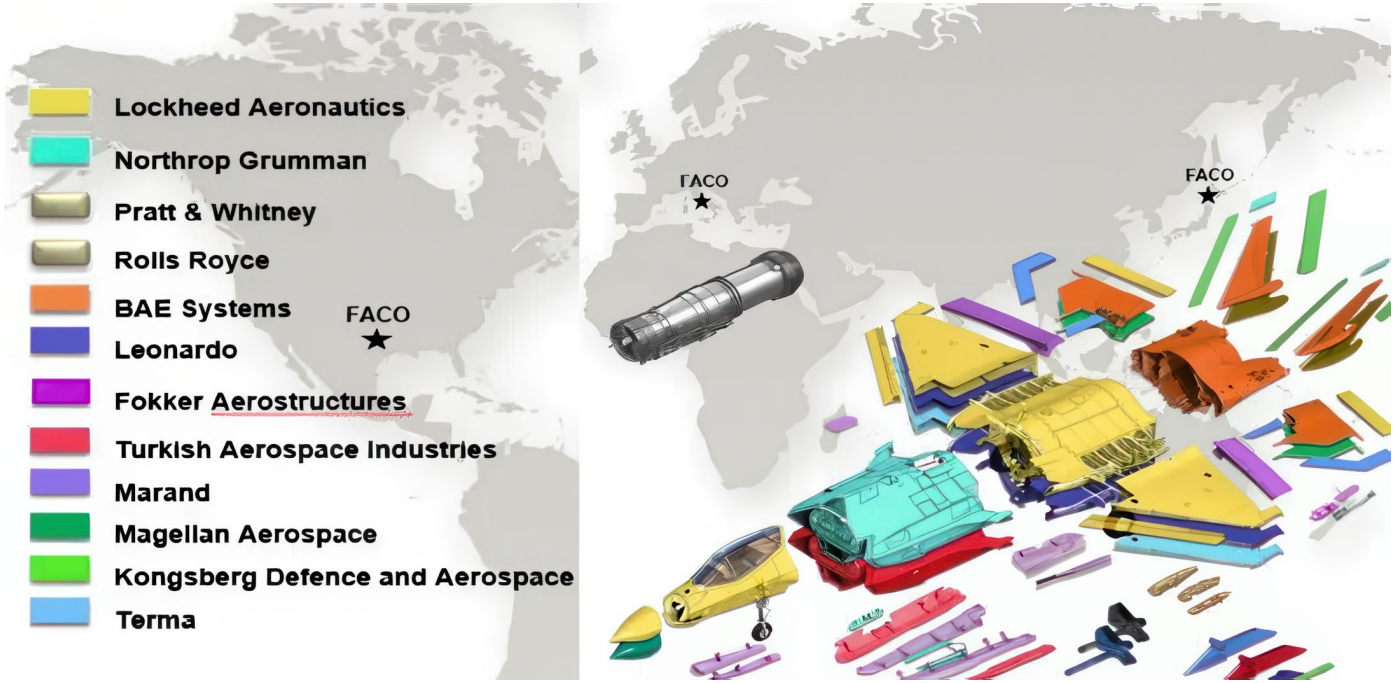


# Global Systemic Risk

## Attributes

- Tightly Coupled Interactions
  - Increased risk of catastrophic failures
- Continuous Flow of Data, Information, Artifacts, Services, People
- Efficiency (E) vs Resiliency (R)
  - Integration vs Dependency
  - Redundancy vs Survivability
  - Stability vs Fragility vs Speed

## F-35 Component Ecosystem



# Systemic Cyber Risks

## Definition & Attributes

- No agreed-upon definition
- A Complex System of Systems with Global Risk that is Interconnected and Complex.
- Third-Parties Dependencies

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

# Cyber-Related Risks Could Be Substantially Worse Than & Different From Others

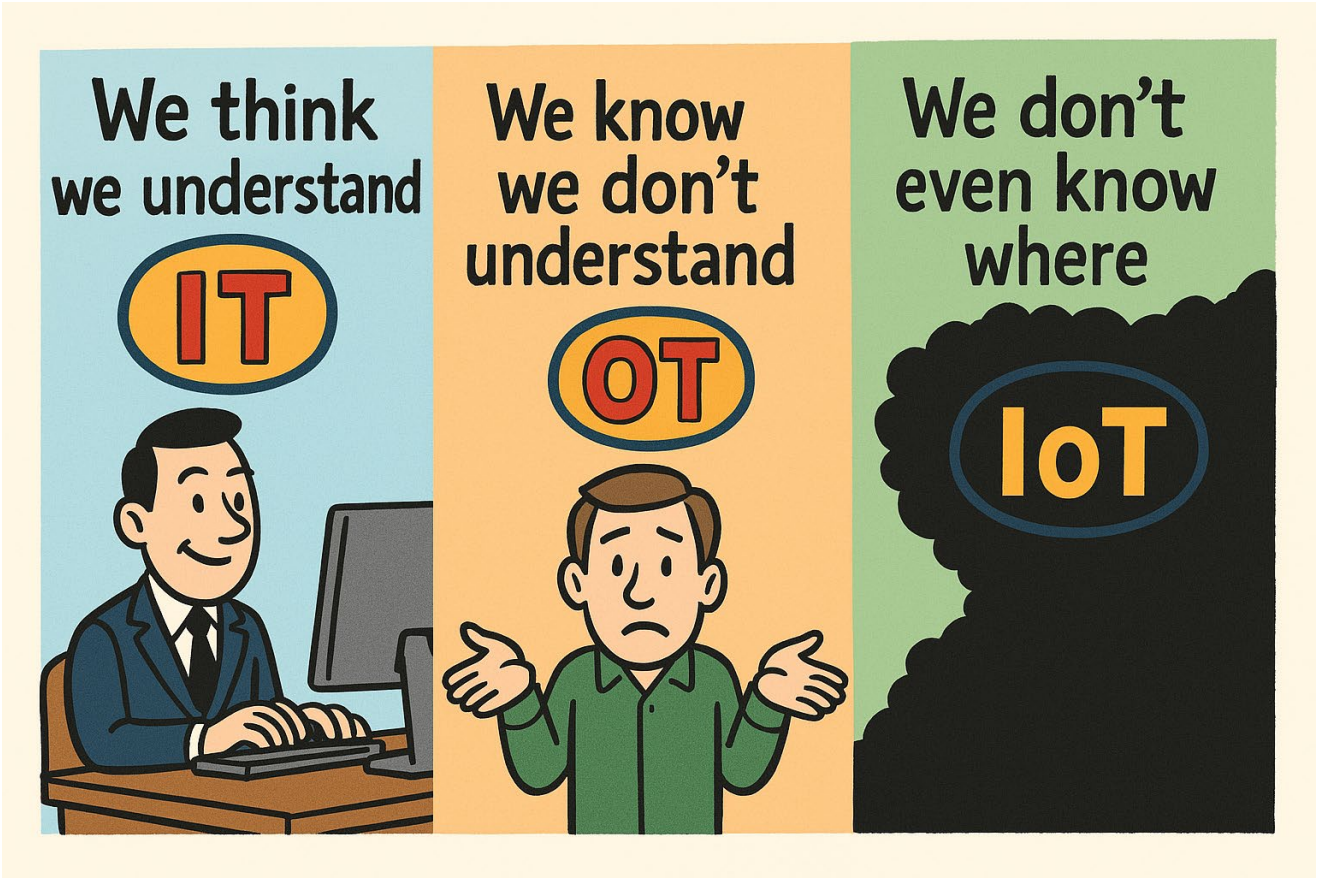
Cyber events can present the worst of all the characteristics of conventional hazards, judged in terms of their onset, duration, visibility, and reach, and can pose even greater challenges than nondigital threats, given the potential for strategic adversaries to inflict harm at low cost and without punishment of repeated attempts.

- Rand Corp. Research Report: Cybersecurity and Supply Chain Risk Management Are Not Simply Additive, © 2023 RAND Corporation

# Systemic Cyber Risks

## Types of Cyber Risk

- Individual vs. Systemic
- Operational, technical, and reputational risks
- IT, IoT, OT / ICS
- Risk Profiles Across Organizational Departments, Functions, and Processes



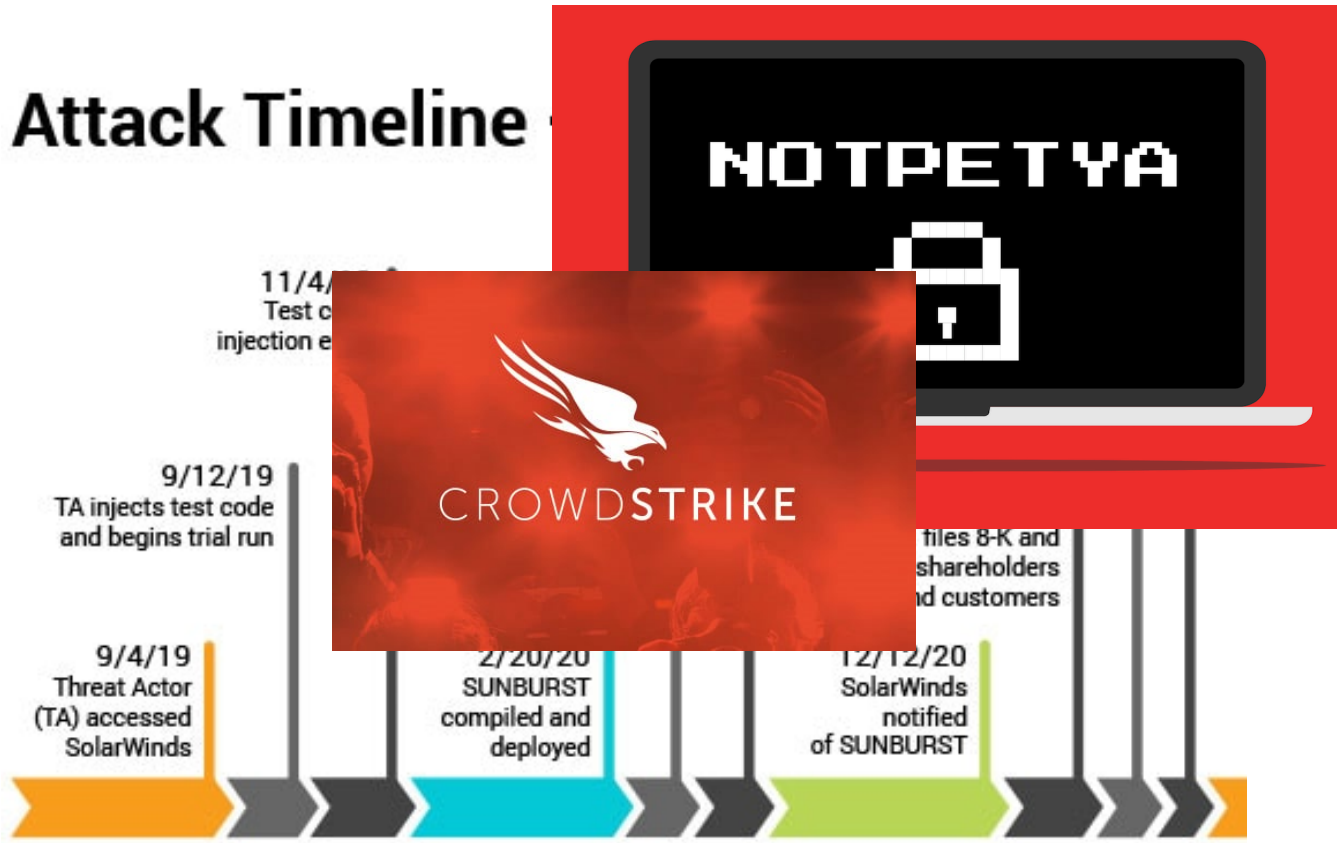
# Do We Understand Our Supply Chain?

- How many links are in your supply chains?
- What planning have you done if a critical small to medium supplier, far down the supply chain has a failure?
- A cyber attack impacts all the supplier's customers and their customers…
- When the 400m-long Ever Given container ship ran aground in March 2021, it paralyzed a critical trade artery for six days, halting hundreds of vessels in a shock that rippled worldwide.
- Toyota had to shut down all their plants in Japan when a plastic parts and electronic components supplier was hit with ransomware.

# Categories of Systemic Cyber Risk

- Vertical Cyber Risk
  - Chain Reaction
  - Attackers hitting an exchange point
- Horizontal Cyber Risk
  - Contagion
  - A flaw in widely used code
- Hybrid Cyber Risk

Not all Risk is an Attack!



# Applying Systems Thinking

## Start with a clear view of Risk

- What you Control, Don't Control, or Don't Know
- Risk Profile = Risk Treatment + Risk Assessment

## Build your Blueprint

- Internal/External Components, Dependencies, and Risk
- Connective Tissue: What to do
- Isolate/segment, Test, 3rd Party

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

# Different Sectors, Different Risk Drivers

Public (GOV), Private, Critical Infrastructure

- Governance & Risk Tolerance Differ
  - Public: Driven by national security, public trust, compliance
  - Private: Driven by profit, brand, customer trust
- Regulatory Environments
- Hybrid Sector: Defense Industrial Base
- The model should reflect your mission and risk priorities.

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

# Tools in Your Kit Bag

## Start with proven frameworks

Use existing models

- FAIR
- NIST Cybersecurity Framework
- CMMC
- MITRE ATT&CK
- DiRECTOR (DDN)

# Identifying Systemic Cyber Risk

## Identify Interconnected& Concentrated Risks

- Expose Systemic Weaknesses
  - Scenario Exercises
  - Test to Failure
  - Stress Test
- Mitigate Cascading Failures
  - Detect before it spreads
  - Have a plan to respond

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

# Mitigating Systemic Cyber Risk

## Key Principles

- Identify & Quantify Value at Risk
- Design for Modularity & Resiliency
- Implement Layered Security
- Implement Feedback Loops
- Zero Trust (obligatory)
- Leverage Information Sharing & Partnerships

Colonial Pipeline Example:

In May 2021, the Colonial Pipeline, a major fuel pipeline, experienced a ransomware attack, causing a temporary shutdown and fuel shortages, highlighting the vulnerability of critical infrastructure to cyberattacks.

They had to shut down the pipeline because without modularity in their architecture, they could not isolate the affected systems from the enterprise network to keep operating.

"This is a common and complex problem in smart manufacturing, and I am afraid not enough manufacturers have thought it through."

- Dawn Cappelli, Head of OT-CERT & former CISO Rockwell Automation

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

# Risk Validation and Verification

Have a clear objective in mind

- Define Success w/ Clear Metrics
- Key Roles for Validation
  - GRC
  - Auditing
- Key Roles for Verification
  - Red Team
- Continuous Monitoring

# Call to Action

## Start Small: You Can't Do It All at Once

- Pick a model - Don't invent your own
- Inventory your assets
- Know your architecture
- Map your ecosystem
- Clarify what you're protecting
- Regular system audits and risk assessments
- Robust incident reporting
- Exercise! Exercise! Exercise!

DOCENT INSTITUTE

EXECUTIVE SECURITY ADVISORS

# Apply What You Have Learned Today

- Stay informed/Listen to the experts. Pay ongoing attention to technological advances, and other global issues.
- Identify and understand your organization's systemic risk.
- Perform Threat Modeling and explore "What If?" scenarios.
- Identify where your weaknesses exist.
- Introduce feedback loops or early warning systems.
- Invest in resiliency to avoid cascading failures, leading to global systemic collapse.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.”

- Sun Tzu

RSAC 2025 Conference

# THANK YOU!

Questions?